At page 4, line 15, insert the following paragraph:

More particularly, the invention is directed to a system for increasing data access in a secure socket layer network environment. The system includes a web server computer having SSL protocol server software operably associated therewith for enabling a SSL connection, wherein SSL protocol server software includes a CA certificate and private key, SSL acceleration server software operably associated with the web server computer which includes a pseudo CA certificate and access to the private key and a public key. A client computer is communicatively linked to the web server computer having web browser software having SSL protocol client software operably associated therewith for enabling a first SSL connection between the client computer and the web server computer, SSL acceleration client software operably associated with the client computer which communicates with the SSL acceleration server software to receive a copy of the pseudo CA certificate and the public key and present the pseudo CA certificate to the web browser software for validation thereof for enabling a second SSL connection between the client computer and the web server computer in a manner which permits optimization techniques to be applied on data transmitted through the second SSL connection.

At page 6, lines 2-22, page 7, lines 1-22 and page 8, lines 1-2 of the filed Specification, please amend the paragraphs as follows:

The present invention is generally depicted in FIGS. 2A and 2B and is directed to a system and method for increasing data access in a secure socket layer network environment and is generally designated by the number 1100 ~~100~~. The system 1100 ~~100~~

includes a web server computer 1102 ~~102~~ which has an operating system/software, server software, memory and linking devices as is known in the art. Further, the computer 1102 ~~102~~ has SSL protocol server software operably disposed thereon for enabling a SSL connection, wherein SSL protocol server software includes a CA certificate and private key.

A client computer 1104 ~~104~~ includes an operating system/software, web browser software having SSL protocol client software operably disposed thereon for enabling a SSL connection, memory and linking devices as is known in the art and is communicatively linked to the web server computer 1102 ~~102~~. SSL acceleration client (SSLAC) software is operably disposed on the client computer 1104 ~~104~~ for monitoring when the web browser requests a SSL connection with the web server 1102 ~~102~~.

SSL acceleration server (SSLAS) software is operably disposed on the web server computer 1104 ~~104~~ for receiving a request for a SSL connection through SSL acceleration client software. The SSL acceleration server software is operably associated with the SSL protocol server software to obtain one either a copy or an equal credential of the CA certificate (i.e., a pseudo CA certificate) and private key.

The operation of the invention can be understood from steps shown in FIGS. 2A and 2B. SSL acceleration client software intercepts 200 new SSL request for a SSL secure connectionfrom the web browser to a target web server. The SSL acceleration client software then initiates 202 a SSL handshake with the SSLAS operably associated with the target web server computer and to start SSL connection. By virtue of the foregoing, a first SSL connection is established between the client and the web server.

The SSLAS then determines 204 which CA certificate is operably associated with the target web server. As part of the SSL handshake between SSLAC and SSLAS, the SSLAS sends 206 this CA certificate to SSLAC along with a public key. At this point a secure SSL session is established between SSLAC and SSLAS and all subsequent data traffic between SSLAC and SSLAS flows over this secure connection. The SSLAC software sends 208 the copy of the CA certificate to the web browser for validation 210. Web browser software sends 212 a list of available encryption algorithms (ciphers) back to target web server (i.e., server computer 1102 ~~102~~). SSLAC software intercepts this from the browser and sends 214 a chosen cipher to the browser software. The web browser software creates 216 a secret key, encrypts using chosen cipher and using the previously received public key and sends 218 the encrypted secret key to the target server, which is intercepted and sent 219 through the SSL acceleration client software to the SSLAS software. SSLAS software de-encrypts 220 the secret key using the private key operably associated with the target server. SSLAS software sends 222 decrypted secret key back to SSLAS software via the secure SSL connection, wherein a "handshake" is completed and secure communications between the client computer's web browser and SSLAS software and by using the secret key, data can be accelerated between the client computer 1104 ~~104~~ and the web server computer 1102 ~~102~~ employing acceleration software, such as compression software of the SSL acceleration client/server software.

Because the SSL connection is terminated by SSLAC, SSLAC can process the data in unencrypted form allowing it to apply data compression and other optimization techniques to the data stream. By virtue of the foregoing, a second SSL connection is

established between the client and web server in a manner which permits optimization techniques to be applied through the second SSL connection. This is done in such a way that the credentials of the SSLAS are presented to the web browser without having violated the SSL paradigm because the private key of the SSLAS was never transmitted to SSLAC.